ABSTRACT

A code computing apparatus with an error detection code (CRC) generating function and an elliptic curve cryptography (ECC) function, comprising a matrix element computation part 30 for generating matrix elements from parameter values set in first and second registers 201 and 202, a matrix element register 51 for holding the matrix elements generated by the matrix element computation part, and an inner product calculation part 40 for executing inner product calculation between the matrix elements held by the matrix element register and data set in a third register. The matrix element computation part selectively generates matrix elements for error detection and matrix elements for encryption by changing the parameters to be set in the first and second registers, and the inner product calculation part is shared to error control code generation and data encryption by altering the matrix elements to be held in the matrix element register.